UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,564	10/10/2003	Keith Woodard	PED-001	9439

21323 7590 05/18/2007

TESTA, HURWITZ & THIBEAULT, LLP
HIGH STREET TOWER
125 HIGH STREET
BOSTON, MA 02110

EXAMINER	
BAYARD, DJENANE M	

ART UNIT	PAPER NUMBER
2141	

MAIL DATE	DELIVERY MODE
05/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/683,564	WOODARD ET AL.	
	Examiner	Art Unit	
	Djenane M. Bayard	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-25,27-34 and 36-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12-25,27-34 and 36-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to communication filed on 2/20/07 in which claims 1-10, 12-25, 27-34 and 36-46 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-10, 12-25, 27-34 and 36-46 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-4, 6-10, 12, 14-18, 20-24, 31, 36, 38, 41 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0212779 to Boyter et al in view of U.S. Patent Application No. 2005/0015760 to Ivanov et al.

a. As per claim 1 and 15, Boyter et al teaches a system and method for network security scanning. Furthermore, Boyter et al teaches a method for scanning network devices connected to a network, comprising: (a) detecting connection of a first network device to the network (See page 4, paragraph [0024], *when a new host, or a new port on an existing host is found it is placed at the top of the priority list to be scanned immediately*); However, Boyter et al fails to teach performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings therefrom, the remote agentless scanning being performed automatically in response to detection of the first network device to thereby avoid downloading a software agent to the first network device; (c) comparing the internal security settings determined through the remote agentless scanning with predefined settings to determine compliance therewith; and (d) automatically performing a remote installation of a security software program on the first network device if the internal security settings are not in compliance with the predefined network settings.

Ivanov teaches automatic detection and patching of vulnerable files. Furthermore, Ivanov teaches wherein a scan-patch module thus searches binary files on client computer to determine if a binary signature identifying security vulnerability is present in any binary information located on client computer. If the bit pattern of the binary signature is found in a binary file , scan-patch module operates to fix the security vulnerability in the binary file by

installing a corresponding security patch on client computer. Installation of a security patch on client computer overwrites or otherwise eliminates the binary file or a portion of the binary file containing the security vulnerability (See page 3, paragraph [0033]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Ivanov in the claimed invention of Boyter et al in order to implement patching of security vulnerabilities in program file in an automatic, comprehensive, reliable and regression free manner (See page 1, paragraph [0008]).

b. As per claim 2, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein step (a) further comprises inspecting data packets communicated over the network (See page 2, paragraph [0012]))

c. As per claims 3, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein the detecting step further comprises querying a database (See page 2, paragraph [0012], *accessing a control database for determining designated address, storing the status of each active host and inactive host in the control database*).

d. As per claim 4, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches broadcasting pings on the network, continuously examining address resolution protocol tables, continuously monitoring event logs, transmitting a Lightweight Directory Access Protocol (LDAP) query, and transmitting a Domain

Name System query (See page 10)

e. As per claim 6, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein step (b) further comprises determining a property of the first network device (See page 9, paragraph [0053]).

f. As per claim 7, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein step (b) further comprises determining an identity of the first network device (See page 9, paragraph [0053]).

g. As per claim 8, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein the determining of the identity of the first network device further comprises at least one of querying a database where the type has been determined, examining network traffic, analyzing network behavior, probing the first network device for signature responses, attempting to log into the device using a series of protocols, logging into the first network device and querying data within the device (See page 2, paragraph [0012] and page 5, paragraph [0031]).

h. As per claim 9, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches scanning at least one of a configuration, file, data, a software version, a patch, inventory, hardware, and a security vulnerability of the first network device (See page 5, paragraph [0031]).

i. As per claim 10, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al wherein step (b) further comprises updating at least one of a configuration, file, data, a software version, inventory, and a security vulnerability of the first network device (See page 2, paragraph [0012] and page 5, paragraph [0031]).

j. As per claim 12, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein step (b) further determining if the first network device is part of a windows domain (See page 3, paragraph [0021] and page 9, paragraph [0053]).

k. As per claims 14 and 20, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches at least one of setting a security policy on the first network device, auditing the security policy of the first network device, ensuring compliance with a predetermined security policy, and reporting result (See page 5, paragraph [0031]).

l. As per claim 16, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches in view of Watkins et al fails to teach wherein the detecting module continuously polls a database for data corresponding to newly attached network devices (See page

m. As per claim 17, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein the scanning module remotely scans the first network device upon detecting data corresponding to the first network device in the database (See page 4, paragraph [0027]).

n. As per claim 18, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches a history database storing scan results of a scan performed by the scanning module (See page 5, paragraph [0031]).

o. As per claim 21, Boyter et al teaches a method for examining a first network device connected to a network, comprising: (a) querying a database for data representing connection of network devices to a network (See page 2, paragraph [0012](b) determining connection of a first network device to the network by locating data about the first network device in the database (See page 2, paragraph [0012] and page 6, paragraph [0012]) (c) determining properties associated with the first network device to determine the identity of the first network device (See pages 4 and 5, paragraph [0028] and page 9, paragraph [0053]); (d) determining items to scan based on at least one of the properties (See page 5, paragraph [0031]); However, Boyter et al fails to teach performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings therefrom, the remote agentless scanning being performed automatically in response to detection of the first network device to thereby avoid downloading a software agent to the first network device.

Ivanov teaches automatic detection and patching of vulnerable files. Furthermore, Ivanov teaches wherein a scan-patch module thus searches binary files on client computer to determine if a binary signature identifying a security vulnerability is present in any binary information located on client computer. If the bit pattern of the binary signature is found in a binary file , scan-patch module operates to fix the security vulnerability in the binary file by installing a corresponding security patch on client computer. Installation of a security patch on client computer overwrites or otherwise eliminates the binary file or a portion of the binary file containing the security vulnerability (See page 3, paragraph [0033]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Ivanov in the claimed invention of Boyter et al in order to implement patching of security vulnerabilities in program file in an automatic, comprehensive, reliable and regression free manner (See page 1, paragraph [0008]).

p. As per claim 22, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein step (c) further comprises determining at least one of credentials associated with the first network device and type of the first network device (See page 4, paragraph [0028] and page 9, paragraph [0053]).

q. As per claim 23, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein step (c) further comprises at least one of querying a database where the identity has already been determined, examining network

traffic, analyzing network behavior, probing the device for signature responses, and logging into the device to query data (See page 2, paragraph [0012]).

r. As per claim 24, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. Furthermore, Boyter et al teaches wherein step (e) further comprises selecting a set of security policy settings to audit (See page 10, paragraph [0055]).

s. As per claims 31 and 36, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al to teach wherein the scanning of internal files and data in step (b) comprises scanning software patch.

Ivanov et al teaches wherein the scanning of internal files and data in step (b) comprises scanning a software patch (See page 3, paragraph [0033]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Ivanov in the claimed invention of Boyter et al in order to implement patching of security vulnerabilities in program file in an automatic, comprehensive, reliable and regression free manner (See page 1, paragraph [0008]).

t. As per claims 38 and 41, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al fails to teach wherein automatically performing a remote installation of a security software program in step (d) comprises installing a new version of the software patch.

Ivanov et al teaches wherein automatically performing a remote installation of a security software program in step (d) comprises installing a new version of the software patch (See page3, paragraph [0033]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Ivanov in the claimed invention of Boyter et al in order to implement patching of security vulnerabilities in program file in an automatic, comprehensive, reliable and regression free manner (See page 1, paragraph [0008]).

u. As per claim 44, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al fails to teach comparing the internal security settings determined through the remote agentless scanning of internal files and data with predefined security settings to determine compliance therewith.

Ivanov et al teaches comparing the internal security settings determined through the remote agentless scanning of internal files and data with predefined security settings to determine compliance therewith (See page 4, paragraph [0044]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Ivanov in the claimed invention of Boyter et al in order to implement patching of security vulnerabilities in program file in an automatic, comprehensive, reliable and regression free manner (See page 1, paragraph [0008]).

5. Claims 27-30 and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0212779 to Boyter et al in view of U.S. Patent Application No. 2005/0015760 to Ivanov et al as applied to claim 1 above, and further in view of U.S. Patent No. 6, 993448 to Tracy et al.

a. As per claim 27 and 33, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al in view of Ivanov et al fails to teach wherein the scanning of internal files and data in step (b) comprise scanning a stored configuration of hardware and software on the first network device.

Tracy et al teaches wherein the scanning of internal files and data in step (b) comprise scanning a stored configuration of hardware and software on the first network device (See col. 7, lines 53-58).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Tracy et al in the claimed invention of Boyter et al in view of Ivanov et al in order to automate the network configuration data collection process of performing security risk assessment (See col. 1, lines 65-67 and col. 2, lines 1-2).

b. As per claims 28 and 29, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al in view of Ivanov fails to teach wherein the scanning of internal files and data in step (b) comprises scanning for incorrectly configured hardware and software.

Tracy et al teaches wherein the scanning of internal files and data in step (b) comprises scanning for incorrectly configured hardware and software (See col. 15, lines 7-43).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Tracy et al in the claimed invention of Boyter et al in view of Ivanov in order to automate the network configuration data collection process of performing security risk assessment (See col. 1, lines 65-67 and col. 2, lines 1-2).

c. As per claims 30 and 34, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al in view of Ivanov fails to teach wherein the scanning of internal files and data in step (b) comprises scanning to determine a software version.

Tracy et al teaches wherein the scanning of internal files and data in step (b) comprises scanning to determine a software version (See col. 7, lines 26-30).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Tracy et al in the claimed invention of Boyter et al in view of Ivanov in order to automate the network configuration data collection process of performing security risk assessment (See col. 1, lines 65-67 and col. 2, lines 1-2).

6. Claims 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0212779 to Boyter et al in view of U.S. Patent Application No. 2005/0015760 to Ivanov et al as applied to claim 1 and 15 above, and further in view as applied

to claim 1 above, and further in view of U.S. Patent Application No. 2001/0047401 to Moore et al.

a. As per claim 5, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al in view of Ivanov et al fails to teach wherein step (b) further comprises determining at least one of whether the first network device is plugged into a wall socket, whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via a Virtual Private Network.

Moore et al teaches a system and methods for determining the physical location of a computer's network interface. Furthermore, Moore et al teaches determining at least one of whether the first network device is plugged into a wall socket, whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via a Virtual Private Network (See page 9, paragraph [0111]).
It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate determining at least one of whether the first network device is plugged into a wall socket, whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via a Virtual Private Network as taught by Moore et al in the claimed invention of Boyter et al in view of Ivanov et al in order to determine the connectivity type of the networks (See page 9, paragraph [0112]

7. Claims 13, 19 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0212779 to Boyter et al in view of U.S. Patent Application No.

2005/0015760 to Ivanov et al as applied to claim 1 and 15 above, and further in view of U.S. Patent Application No. 2004/0268145 to Watkins et al.

a. As per claims 13, 19 and 25, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al in view of Ivanov et al fails to teach at least one of enabling the first network device to have additional access to the network, denying the first network device access to the network, notifying another about the first network device based on results of the scan, and quarantining the first network device.

Watkins et al teaches one of enabling the first network device to have additional access to the network, denying the first network device access to the network, notifying another about the first 1, paragraph [0009], *the results of these checks are returned via the web and are used for security decisions involving the granting of authorization to access network services*).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate at least one of enabling the first network device to have additional access to the network, denying the first network device access to the network, notifying another about the first network device based on results of the scan, and quarantining the first network device as taught by Watkins et al in the claimed invention of Chari et al in order to provide a reliable client integrity scheme that can consistently regulate access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

8. Claims 32 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0212779 to Boyter et al in view of U.S. Patent Application No. 2005/0015760 to Ivanov et al as applied to claim 1 and 15 above, and further in view as applied to claims 1 and 15 above, and further in view of U.S. Patent No. 6, 546493 to Magdych et al.

a. As per claim 32 and 37, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al in view of Ivanov et al fails to teach wherein the scanning of internal files and data in step (b) comprises scanning for viruses.

Magdych et al teaches a system and method for risk assessment scanner. Furthermore, Magdych et al teaches wherein the scanning of internal files and data in step (b) comprises scanning for viruses (See col. 3, lines 35-49, col. 5, lines 61-67, col. 6, lines col. 1, lines 60-67).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Magdych into the claimed invention of Boyter et al in view of Ivanov et al in order to identify the vulnerabilities as the source (See col. 2, lines 30-31).

9. Claims 39, 42 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0212779 to Boyter et al in view of U.S. Patent Application No. 2005/0015760 to Ivanov et al as applied to claim 1 and 15 above, and further in view as applied to claims 1 and 15 above, and further in view of U.S. Patent Application No. 2005/0050335 to Liang et al.

a. As per claims 39, 42 and 45, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al in view of Ivanov et al fails to teach wherein the scanning of internal files and data in step (b) comprises searching for a predetermined anti-virus software, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the predetermined anti-virus software if the predetermined anti-virus software is not found in step (b).

Liang et al teaches comprises searching for a predetermined anti-virus software, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the predetermined anti-virus software if the predetermined anti-virus software is not found in step (b) (See page 5, paragraph [0054-0055]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Liang et al in the claimed invention of Boyter et al in view of Ivanov et al in order to provide the client device with the appropriate anti-virus software (See page 5, paragraph [0054]).

10. Claims 40, 43 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0212779 to Boyter et al in view of U.S. Patent Application No. 2005/0015760 to Ivanov et al as applied to claim 1 and 15 above, and further in view as applied to claims 1 and 15 above, and further in view of U.S. Patent Application No. 2006/0010492 to Heintz et al.

a. As per claims 40, 43 and 46, Boyter et al in view of Ivanov et al teaches the claimed invention as described above. However, Boyter et al in view of Ivanov et al fails to teach wherein the scanning of internal files and data in step (b) comprises determining whether firewall software is installed, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the firewall software if it is determined in step (b) that the firewall software has not yet been installed.

Heintz et al teaches wherein the scanning of internal files and data in step (b) comprises determining whether firewall software is installed, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the firewall software if it is determined in step (b) that the firewall software has not yet been installed (See page 2, paragraph [0024]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Heintz et al in the claimed invention of Boyter et al in view of Ivanov et al in order to monitor the activity of a user on a network component (See page 1, paragraph [0009]).

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Djenane M. Bayard whose telephone number is (571) 272-3878. The examiner can normally be reached on Monday- Friday 5:30 AM- 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Djenane Bayard

Patent Examiner

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER